AMENDMENTS TO THE CLAIMS

This listing of claims replaces all prior versions, and listings, of claims in the application:

Listing of Claims:

1. (Currently Amended) At a computer system including system memory and one or more processors, the computer system connected to one or more other computer systems via a computer network, the computer system also including a distributed application component of a distributed application, one or more other distributed application components of the distributed application being included at the one or more other computer systems, the distributed application component and the one or more other distributed application components configured to interoperate to implement the functionality of the distributed application, the computer system and each of the one or more other computer systems having computer system measurable aspects indicating a configuration for use in machine authentication, the component and each of the one or more other components of the distributed application having application measurable aspects indicating a configuration for use in application authentication, ~~At a module having at least one measurable aspect, the module being communicatively connectable to a verification module that can verify the authenticity of assertions formulated at other modules~~, a method for providing information that can be used to securely verify measurable aspects of the ~~module~~ distributed application component, the method comprising:

an act of the distributed application component sending communication to another computer system, the other computer system selected from among the one or more other computer systems, the communication requesting access to a resource under the control of another distributed application component of the distributed application that is at the other computer system;

an act of the computer system and the other distributed application component conducting application authentication so that the computer system can verify the identity of the other distributed application component, application authentication including the computer system receiving proof from the other distributed application component that the other distributed application component complies with one or more security policies of the computer system;

an act of ~~accessing an indication~~ the computer system accessing information that indicates how to prove an appropriate configuration, from among one or more appropriate configurations, to access the resource in accordance with the one or more security policies subsequent to and in response to successfully conducting application authentication, the accessed information indicating that one or more application measurable aspects of the ~~module's configuration~~ distributed application component and one or more computer system measurable aspects of the computer system are to be verified to prove that the combination of the distributed application component and the computer system provide an appropriate configuration to interoperate with the other distributed application component to access the resource;

an act of the processor formulating an assertion that can ~~be~~ used to verify the one or more application measurable aspects and the one or more computer system measurable aspects, the assertion representing identity values for the one or more application measureable aspects and representing environment values for the one or more computer system measurable aspects, the identity values expressly indicating the identity and the functionality of portions of computer-executable instructions included the distributed application component, the environment values identifying the execution environment at the computer system ~~that the module is configured in accordance with the one or more measurable aspects~~; and

an act of sending the formulated assertion for verification.

Claim 2. (Cancelled).

3. (Currently Amended) The method as recited in claim 1, further comprising:

an act of receiving a request for proof that the ~~module~~ distributed application component and the computer system ~~is~~ are appropriately configured to interoperate with the other distributed application component to access the resource ~~issue challenges to a requesting module~~, the request being received prior to accessing information that indicates how to prove an appropriate configuration ~~the indication that one or more measurable aspects of the module's configuration are to be verified~~.

4. (Currently Amended) The method as recited in claim 1, wherein the act of accessing information that indicates how to prove an appropriate configuration ~~indication is~~ comprises an act of accessing administrative policies associated with the resource.

5. (Currently Amended) The method as recited in claim 1, wherein act of accessing information that indicates how to prove an appropriate configuration ~~the indication is~~ comprises an act of accessing receiving a message from ~~the~~ a verification module.

Claim 6. (Cancelled).

7. (Currently Amended) The method as recited in claim ~~6~~1, wherein the act of accessing information that indicates how to prove an appropriate configuration comprises an act of accessing ~~the~~ a request for ~~information is a request for~~ values associated with one or more of an assembly, ~~a SEE application,~~ a hardware component, a platform, an environment variable, a call stack, and a data stream.

8. (Currently Amended) The method as recited in claim 7~~6~~, wherein the request for ~~information is~~ values comprises a request for the values associated with ~~of~~ the one or more application measurable aspects.

9. (Currently Amended) The method as recited in claim 8, wherein the request for the values of the one or more application measurable aspects comprises a request for the identity of one or more portions of executable instructions at the requester.

10. (Currently Amended) The method as recited in claim ~~8~~1, wherein the act of accessing information that indicates how to prove an appropriate configuration comprises an act of accessing ~~the request for the values of the one or more measurable aspects is~~ a request for byte values included in the computer-executable instructions of a specified version of the distributed application. ~~the values of the one or more measurable aspects of an execution environment at the requester~~.

Claim 11. (Cancelled) .

12. (Currently Amended) The method as recited in claim ~~11~~6, wherein the act of accessing information that indicates how to prove an appropriate configuration comprises an act of a accessing a request for a digest of the one or more application measurable aspects.

Claims 13 and 14 (Cancelled).

15. (Currently Amended) The method as recited in claim 1, wherein the assertion is formulated proof that can be used to verify byte values included in the computer-executable instructions of a specified version of the distributed application ~~the identity of one or more portions of executable instructions~~.

Claim 16. (Cancelled).

17. (Currently Amended) The method as recited in claim 1~~6~~, wherein the ~~formulating proof~~ assertion is formulated proof that the ~~module~~ distributed application component is to execute in a compartmentalized environment.

18. (Currently Amended) The method as recited in claim 1~~6~~, wherein the ~~formulated proof of~~ assertion is formulated proof that the ~~module~~ distributed application component has access to one or more of an assembly, ~~a SEE application,~~ a hardware component, a platform, an environment variable, a call stack, or a data stream.

Claim 19. (Cancelled).

20. (Currently Amended) The method as recited in claim 1~~9~~, wherein the assertion ~~formulated representation~~ is a digest representing the values of the one or more application measurable aspects.

21. (Currently Amended) The method as recited in claim 1, wherein the assertion is formulated proof that indicates at least one: of compliance with one or more required policies or ~~a providing module,~~ that ~~the module~~ distributed application component is not a virus, or ~~and~~ that the ~~module~~ distributed application component is not an intruder.

22. (Currently Amended) The method as recited in claim 1, wherein the assertion is formulated proof that the distributed application component~~module~~ is configured in accordance with at least one pre-determined configuration.

23. (Currently Amended) The method as recited in claim 1, further comprising:

an act of digitally signing the assertion~~formulated proof~~.

24 (Currently Amended) The method as recited in claim 23, wherein the assertion is signed using a private key as proof ~~is signed using a private key~~ that the assertion can be validated by a group public key~~also able to validate at least one other private key~~.

25. (Currently Amended) The method as recited in claim 23, wherein the ~~proof~~ assertion is signed using a per-machine key that identifies the module.

26. (Currently Amended) The method as recited in claim 23, wherein the ~~proof~~ assertion is signed using a zero knowledge algorithm.

27. (Currently Amended) The method as recited in claim 23, wherein the ~~proof~~ assertion is signed using a hardware-based key.

28. (Currently Amended) The method as recited in claim 23, wherein the ~~proof~~ assertion is signed using a communication channel key.

29. (Currently Amended) The method as recited in claim 23, wherein the act of digitally signing the formulated proof comprises an act of digitally signing ~~data~~ bytes taken from

one or more identified code regions of computer-executable instructions within ~~in~~ the distributed application~~module~~.

30. (Original) The method as recited in claim 1, wherein the act of sending the formulated assertion to the verification module comprises sending the formulated assertion to a token service.

31. (Currently Amended) The method as recited in claim 1, further comprising:

an act of receiving a token that represents proof that the combination of the distributed application component and the computer system are appropriately configuration to interoperate with the other distributed application component to access the resource~~one or more measurable aspects have been verified~~.

32. (Currently Amended) The method as recited in claim 1, ~~further comprising:~~ wherein

~~an act of downloading a list of~~ the one or more appropriate configurations are ~~that~~ have been pre-determined to be appropriate for accessing the~~a~~ resource.

33. (Withdrawn) At a module communicatively connectable to another module that can send assertions to the module, a method for verifying that the other module is configured in accordance with one or more measurable aspects, the method comprising:

an act of providing an indication that one or more measurable aspects of the other module's configuration are to be verified;

an act of receiving an assertion that can be used to verify that the other module is configured in accordance with the one or more measurable aspects; and

an act of verifying the assertion.

34. (Withdrawn) The method as recited in claim 33, further comprising:

an act of receiving a request to access a resource of the module prior to providing the indication of the one or more measurable aspects of the other module's configuration that are to be verified.

35. (Withdrawn) The method as recited in claim 33, further comprising:

an act of sending a request for proof that the other module is appropriately configured to issue challenges to the module, the request being sent prior providing the indication of the one or more measurable aspects of the other module's configuration that are to be verified.

36. (Withdrawn) The method as recited in claim 33, wherein the indication is a challenge that requests information that allows the one or more measurable aspects to be verified.

37. (Withdrawn) The method as recited in claim 36, wherein the challenge requests proof of the values of one or more measurable aspects.

38. (Withdrawn) The method as recited in claim 37, wherein the challenge requests a representation of the values of the one or more measurable aspects.

39. (Withdrawn) The method as recited in claim 38, wherein the challenge requests a digest of the one or more measurable aspects.

40. (Withdrawn) The method as recited in claim 36, wherein the challenge requests proof of the identity of one or more portions of executable instructions.

41. (Withdrawn) The method as recited in claim 36, wherein the challenge requests proof an execution environment.

42. (Withdrawn) The method as recited in claim 33, wherein the assertion includes the identity of one or more portions of executable instructions.

43. (Withdrawn) The method as recited in claim 33, wherein the assertion includes the values of one or more measurable aspects of an execution environment.

44. (Withdrawn) The method as recited in claim 43, wherein the assertion indicates that the other module has access to one or more of an assembly, a SEE application, a hardware component, a platform, an environment variable, a call stack, and a data stream.

45. (Withdrawn) The method as recited in claim 43, wherein the assertion is a representation of the values of one or more measurable aspects of the requester.

46. (Withdrawn) The method as recited in claim 45, wherein the assertion is a digest of the values of one or more measurable aspects of the requester.

47. (Withdrawn) The method as recited in claim 33, wherein the assertion indicates that the other module is executing in a compartmentalized resource.

48. (Withdrawn) The method as recited in claim 33, wherein the assertion indicates at least one of compliance with one or more administrative policies, that the other module is certified to access a resource of the module, that the other module is not a virus, that the other module is not infected with a virus, that the other module is not an intruder, and that the other module is appropriately configured to issue challenges to the module.

49. (Withdrawn) The method as recited in claim 33, wherein the assertion is a token issued from a token service.

50. (Withdrawn) The method as recited in claim 33, wherein the assertion indicates that the other module is configured in accordance with at least one pre-determined configuration.

51. (Withdrawn) The method as recited in claim 33, wherein the assertion is verified using a group public key that corresponds to a plurality of private keys.

52. (Withdrawn) The method as recited in claim 33, wherein the assertion is verified using a zero knowledge algorithm.

53. (Currently Amended) A computer program product for use in a computer~~ing~~ system, the computer system connected to one or more other computer systems via a computer network, the computer system also including a distributed application component of a distributed application, one or more other distributed application components of the distributed application being included at the one or more other computer systems, the distributed application component and the one or more other distributed application components configured to interoperate to implement the functionality of the distributed application, the computer system and each of the one or more other computer systems having computer system measurable aspects indicating a configuration for use in machine authentication, the component and each of the one or more other components of the distributed application having application measurable aspects indicating a configuration for use in application authentication, ~~with a module having at least one measurable aspect, the module being communicatively connectable to a verification module that can verify the authenticity of assertions formulated at other modules,~~ the computer program product for implementing a method for providing information that can be used to securely verify measurable aspects of the~~ module~~ distributed application component, the computer program product comprising one or more computer-readable storage media having stored thereon computer-executable instructions that, when executed by a processer~~d~~, cause the computer system to perform the method, including following:

send communication to another computer system, the other computer system selected from among the one or more other computer systems, the communication requesting access to a resource under the control of another distributed application component of the distributed application that is at the other computer system;

conduct application authentication with the other distributed application component so that the computer system can verify the identity of the other distributed application component, application authentication including the computer system receiving proof from the other distributed application component that the other distributed application component complies with one or more security policies of the computer system;

~~access an indication~~ the computer system accessing information that indicates how to prove an appropriate configuration, from among one or more appropriate configurations, to access the resource in accordance with the one or more security policies subsequent to and in response to successfully conducting application authentication, the accessed information indicating that one or more application measurable aspects of the ~~module's configuration~~ distributed application component and one or more computer system measurable aspects of the computer system are to be verified to prove that the combination of the distributed application component and the computer system provide an appropriate configuration to interoperate with the other distributed application component to access the resource;

formulate an assertion that can ~~be~~ used to verify the one or more application measurable aspects and the one or more computer system measurable aspects, the assertion representing identity values for the one or more application measureable aspects and representing environment values for the one or more computer system measurable aspects, the identity values expressly indicating the identity and the functionality of portions of computer-executable instructions included the distributed application component, the environment values identifying the execution environment at the computer system ~~that the module is configured in accordance with the one or more measurable aspects~~; and

send~~ing~~ the formulated assertion for verification.

54. (Withdrawn) A computer program product for use in a computing system with a module communicatively connectable to another module that can send assertions to the module, the computer program product for implementing a method for verifying that the other module is configured in accordance with one or more measurable aspects, the computer program product comprising one or more computer-readable media having stored thereon computer-executable instructions that, when executed by a processed, cause the computer system to perform the following:

provide an indication that one or more measurable aspects of the other module's configuration are to be verified;

receive an assertion that can be used to verify that the other module is configured in accordance with the one or more measurable aspects; and

verify the assertion.

53. (New) A computer system, the computer system comprising:

system memory;

one or more processors; and

one or more computer-readable media having stored thereon computer-executable instructions representing an application authentication module, a machine authentication module, and a distributed application component of a distributed application, wherein the machine authentication module configured to:

conduct machine authentication with other computer systems, including establishing a Secure Sockets Layer (SSL) connection between the computer system and the other computer systems;

wherein the application authentication module is configured to:

conduct application authentication with distributed application components of the distributed application at other computer systems after the other computer systems have been authenticated using machine authentication so that the computer system can verify the identity of the other distributed application component, application authentication including the computer system receiving proof from the other distributed application components that the other distributed application components comply with one or more security policies of the computer system; and

wherein the distributed application component is configured to:

send communication other computer systems that include a distributed application component for the distributed application, the communication requesting access to a resource under the control of another distributed application component at the other computer system;

access information that indicates how to prove an appropriate configuration, from among one or more appropriate configurations, to access the resource in accordance with the one or more security policies subsequent to and in response to successfully conducting application authentication, the accessed information indicating that one or more application measurable aspects of the distributed application component, including access to specified byte values from within specified locations in computer-executable instructions of the distributed application, and one or more computer system measurable aspects of the computer system, including specified values for specified execution environment variables, are to be verified to prove that the combination of the distributed application component and the computer system provide an appropriate execution environment for interoperating with the other distributed application component to access the resource;

formulate an assertion that can used to verify the one or more application measurable aspects and the one or more computer system measurable aspects, the assertion including the specified byte values from within the specified locations in computer-executable instructions and the specified values for the specified execution environment variables;

send the formulated assertion for verification;

receive a token representing that the combination of the distributed application component and the computer system do provide an appropriate execution environment for interoperating with the other distributed application component to access the resource; and

submit the token to the other computer system so that the other computer system can verify that the combination of the distributed application component and the computer system do provide an appropriate execution environment for accessing the resource based on the context of the token.